

Claims

WHAT IS CLAIMED IS:

1. A method of authenticating an identity of a user seeking access to a relying computing entity, wherein the identity of the user is issued by an authentication service and is not issued by the relying computing entity, the method comprising:

receiving at a broker service an authentication request from the relying computing entity to authenticate the identity of the user, wherein a first trust relationship exists between the relying computing entity and the broker service, and a second trust relationship exists between the authentication service and the broker service, in the absence of a relevant trust relationship existing between the authentication service and the relying computing entity;

receiving an authentication response from the authentication service, responsive to receiving the authentication request at the broker service; and

sending an authentication response from the broker service to the relying computing entity representing a trusted authentication of the identity of the user to the relying computing entity based on the first trust relationship and the second trust relationship.

2. The method of claim 1 further comprising:

sending the authentication request to the authentication service, responsive to receiving the authentication request at the broker service.

1 3. The method of claim 1 further comprising:
2 collecting a credential of the user, responsive to receiving the authentication
3 request at the broker service; and
4 sending the credential to the authentication service for validation by the
5 authentication service.

6 4. The method of claim 1 wherein the credential cannot be interpreted by
7 the broker service.

8 5. The method of claim 1 wherein the broker service and the authentication
9 service are hosted by a single computing system.

10 6. The method of claim 1 wherein the broker service and the authentication
11 services are hosted within a single computing entity.

12 7. The method of claim 1 wherein authentication account information
13 associated with the user and maintained by the authentication service is accessible
14 through an interface to the authentication service.

15 8. The method of claim 1 further comprising:
16 validating based on the first trust relationship that the authentication request
17 was received by the broker service from the relying computing entity.

18 9. The method of claim 1 wherein other computing entities have trust
19 relationships established with the broker service.

1 10. The method of claim 1 wherein the first trust relationship represents an
2 agreement between the broker service and the relying computing entity to comply
3 with one or more brokered authentication rules.

4 11. The method of claim 1 wherein the first trust relationship represents an
5 exchange of one or more security keys between the broker service and the relying
6 computing entity.

7 12. The method of claim 1 wherein the first trust relationship represents an
8 agreement by the relying computing entity to recognize assertions provided by the
9 broker service.
10

11 13. The method of claim 1 wherein the operation of receiving at a broker
12 service an authentication request is responsive to an access request by the user for
13 access to the relying computing entity.

14 14. The method of claim 1 wherein the operation of receiving at a broker
15 service an authentication request comprises:
16

17 receiving the authentication request at the broker service as a redirected
18 message through a computer system of the user.

19 15. The method of claim 1 further comprising:
20 validating a credential received from the user by the authentication service.

21 16. The method of claim 1 further comprising:
22 sending a challenge request to the user, responsive to the operation of
23 receiving at a broker service an authentication request; and
24
25

1 validating a credential received from the user in response to the challenge
2 request.

3 17. The method of claim 1 further comprising:
4 returning a session ticket to the user to allow user access to the relying
5 computing entity.

6 18. The method of claim 1 further comprising:
7 redirecting the user to the authentication service based on an identifier of
8 the user.

9 19. The method of claim 1 further comprising:
10 translating the authentication response received from the authentication
11 service into a protocol recognized by the relying computing entity.
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 20. A computer program product encoding a computer program for
2 executing on a computer system a computer process for authenticating an identity
3 of a user seeking access to a relying computing entity, wherein the identity of the
4 user is issued by an authentication service, the computing process comprising:

5 receiving at a broker service an authentication request from the relying
6 computing entity to authenticate the identity of the user, wherein a first trust
7 relationship exists between the relying computing entity and the broker service,
8 and a second trust relationship exists between the authentication service and the
9 broker service;

10 receiving an authentication response from the authentication service; and

11 sending an authentication response from the broker service to the relying
12 computing entity representing a trusted authentication of the identity of the user to
13 the relying computing entity based on the first trust relationship and the second
14 trust relationship.

15
16 21. The computer program product of claim 20 wherein the computer
17 process further comprises:

18 sending the authentication request to the authentication service, responsive
19 to receiving the authentication request at the broker service.

1 22. The computer program product of claim 20 wherein the computer
2 process further comprises:
3 collecting a credential of the user, responsive to receiving the authentication
4 request at the broker service; and
5 sending the credential to the authentication service for validation by the
6 authentication service.

7 23. The computer program product of claim 20 wherein the credential
8 cannot be interpreted by the broker service.
9

10 24. The computer program product of claim 20 wherein the broker service
11 and the authentication service are hosted by a single computing system.

12 25. The computer program product of claim 20 wherein the broker service
13 and the authentication services are hosted within a single computing entity.
14

15 26. The computer program product of claim 20 wherein authentication
16 account information associated with the user and maintained by the authentication
17 service is accessible through an interface to the authentication service.

18 27. The computer program product of claim 20 wherein the computer
19 process further comprises:

20 validating based on the first trust relationship that the authentication request
21 was received by the broker service from the relying computing entity.
22

23 28. The computer program product of claim 20 wherein other computing
24 entities have trust relationships established with the broker service.
25

1 29. The computer program product of claim 20 wherein the first trust
2 relationship represents an agreement between the broker service and the relying
3 computing entity to comply with one or more brokered authentication rules.

4 30. The computer program product of claim 20 wherein the first trust
5 relationship represents an exchange of one or more security keys between the
6 broker service and the relying computing entity.

7 31. The computer program product of claim 20 wherein the first trust
8 relationship represents an agreement by the relying computing entity to recognize
9 assertions provided by the broker service.
10

11 32. The computer program product of claim 20 wherein the operation of
12 receiving at a broker service an authentication request is responsive to an access
13 request by the user for access to the relying computing entity.

14 33. The computer program product of claim 20 wherein the operation of
15 receiving at a broker service an authentication request comprises:
16

17 receiving the authentication request at the broker service as a redirected
18 message through a computer system of the user.

19 34. The computer program product of claim 20 wherein the computer
20 process further comprises:

21 validating a credential received from the user by the authentication service.
22
23
24
25

1 35. The computer program product of claim 20 wherein the computer
2 process further comprises:
3 sending a challenge request to the user, responsive to the operation of
4 receiving at a broker service an authentication request; and
5 validating a credential received from the user in response to the challenge
6 request.

7 36. The computer program product of claim 20 wherein the computer
8 process further comprises:
9 returning a session ticket to the user to allow user access to the relying
10 computing entity.

11 37. The computer program product of claim 20 wherein the computer
12 process further comprises:
13 redirecting the user to the authentication service based on an identifier of
14 the user.
15

16 38. The computer program product of claim 20 wherein the computer
17 process further comprises:
18 translating the authentication response received from the authentication
19 service into a protocol recognized by the relying computing entity.
20
21
22
23
24
25

1 39. A computer system for authenticating an identity of a user seeking
2 access to a relying computing entity, wherein the identity of the user is issued by
3 an authentication service, the computing system comprising:

4 an authentication broker service having a first trust relationship with the
5 relying computing entity and a second trust relationship with the authentication
6 service, the authentication broker service receiving an authentication request from
7 the relying computing entity to authenticate the identity of the user and receiving
8 an authentication response from the authentication service,

9 the authentication broker service further sending an authentication response
10 to the relying computing entity representing a trusted authentication of the identity
11 of the user to the relying computing entity based on the first trust relationship and
12 the second trust relationship.
13
14
15
16
17
18
19
20
21
22
23
24
25

1 40. A method of establishing a brokerable trust relationship between an
2 authentication broker service and each of a plurality of computing entities, the
3 method comprising:

4 establishing one or more brokered authentication rules governing brokered
5 authentication through the authentication broker service;

6 obtaining an agreement from each computing entity to comply with the one
7 or more brokered authentication rules; and

8 configuring the authentication broker service to authenticate identities of
9 one or more users for each computing entity in accordance with the one or more
10 brokered authentication rules, wherein the one or more users have identities issued
11 by one or more authentication services having trust relationships with the
12 authentication broker service.

13
14 41. The method of claim 40 further comprising:

15 exchanging one or more security keys between the authentication broker
16 service and each of the computing entities.

1 42. A computer program product encoding a computer program for
2 executing on a computer system a computer process for establishing a brokerable
3 trust relationship between an authentication broker service and each of a plurality
4 of computing entities, the computer process comprising:

5 establishing one or more brokered authentication rules governing brokered
6 authentication through the authentication broker service;

7 obtaining an agreement from each computing entity to comply with the one
8 or more brokered authentication rules; and

9 configuring the authentication broker service to authenticate identities of
10 one or more users for each computing entity in accordance with the one or more
11 brokered authentication rules, wherein the one or more users have identities issued
12 by one or more authentication services having trust relationships with the
13 authentication broker service.

14
15 43. The computer program product of claim 42 wherein the computer
16 process further comprises:

17 exchanging one or more security keys between the authentication broker
18 service and each of the computing entities.